Research Article

Thomas W. Cusick and Younhwan Cheon

Theory of 3-rotation symmetric cubic Boolean functions

Abstract: Rotation symmetric Boolean functions have been extensively studied in the last 15 years or so because of their importance in cryptography and coding theory. Until recently, very little was known about such basic questions as when two such functions are affine equivalent. This question in important in applications, because almost all important properties of Boolean functions (such as Hamming weight, nonlinearity, etc.) are affine invariants, so when searching a set for functions with useful properties, it suffices to consider just one function in each equivalence class. This can greatly reduce computation time. Even for quadratic functions, the analysis of affine equivalence was only completed in 2009. The much more complicated case of cubic functions was completed in the special case of affine equivalence under permutations for monomial rotation symmetric functions in two papers from 2011 and 2014. There has also been recent progress for some special cases for functions of degree > 3. In 2007 it was found that functions satisfying a new notion of k-rotation symmetry for $k > 1$ (where the case $k = 1$ is ordinary rotation symmetry) were of substantial interest in cryptography and coding theory. Since then several researchers have used these functions for $k = 2$ and 3 to study such topics as construction of bent functions, nonlinearity and covering radii of various codes. In this paper we develop a detailed theory for the monomial 3-rotation symmetric cubic functions, extending earlier work for the case $k = 2$ of these functions.

Keywords: Boolean functions, rotation symmetry, affine equivalence, equivalence class, Hamming weight, recursions

MSC 2010: 94C10, 94A15, 06E30

Thomas W. Cusick: Department of Mathematics, University at Buffalo, 244 Mathematics Building, Buffalo, NY 14260, USA, e-mail: cusick@buffalo.edu

Younhwan Cheon: Korea Army Academy at Yeong-Cheon, KyungBuk 770-849, Republic of Korea, e-mail: yhcrypt@gmail.com

Communicated by: Tor Helleseth

1 Introduction

Boolean functions have a variety of applications in the field of cryptography, a thorough overview of which can be found in [12]. A Boolean function in n variables can be defined as a map from $\mathbb{V}_n$, the n-dimensional vector space over the two element field $\mathbb{F}_2$, to $\mathbb{F}_2$. If f is a Boolean function in n variables, the *truth table* of f is defined to be the 2^n-tuple given by $(f(\mathbf{v}_0), f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^n-1}))$ where $\mathbf{v}_0 = (0, \ldots, 0, 0), \mathbf{v}_1 = (0, \ldots, 0, 1), \ldots, \mathbf{v}_{2^n-1} = (1, \ldots, 1, 1)$ are the 2^n elements of $\mathbb{V}_n$ listed in lexicographical order. The *weight* or *Hamming weight* of f (notation $\mathrm{wt}(f)$) is the number of 1's that appear in the truth table of f.

As described in [12, pp. 5–6], every Boolean function on $\mathbb{V}_n$ can be expressed as a polynomial over $\mathbb{F}_2$ in n binary variables by

$$f(x_1, \ldots, x_n) = \sum_{\mathbf{a} \in \mathbb{V}_n} c_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}$$

where $c_{\mathbf{a}} \in \mathbb{F}_2$ and $\mathbf{a} = (a_1, \ldots, a_n)$ with each a_i equal to 0 or 1. The above representation is referred to as the *algebraic normal form* (ANF) of f. Let d_i be the number of variables in the i-th monomial of f, so d_i is the *algebraic degree* (or just the *degree*) of the monomial. If we let D be the set of the distinct degrees of the monomials in f which have non-zero coefficients, then the *degree* of f is given by $\max(D)$. If D contains only one element, then each monomial in f has the same degree and f is said to be *homogeneous*. If the degree of f is 1, then f is said to be *affine*, and if f is affine and homogeneous (i.e. the constant term is 0), f is said to be *linear*.

A Boolean function f is said to be *rotation symmetric* if its ANF is invariant under any power of the cyclic permutation $\rho(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1)$. The function is said to be *k-rotation symmetric* if it is invariant under the k-th power of ρ but not under any smaller power (so the number of variables must be divisible by k). A rotation symmetric function (respectively, k-rotation symmetric function) is said to be *monomial rotation symmetric (MRS)* if it is generated by applying powers of ρ (respectively, powers of ρ^k) to a single monomial. The k-rotation symmetric functions were introduced in [18], where they were used to extend the results of [16, 17]. Paper [17] announced that searching the set of rotation symmetric functions had led to the discovery of 9-variable Boolean functions with nonlinearity 241. In the previous 30 years no examples with nonlinearity exceeding 240 had been found. In later work [16] it was possible to show by exhaustive search that no 9-variable rotation symmetric functions with nonlinearity exceeding 241 exist. However, in [18] some functions with nonlinearity 242 were found by searching a subset of the 9-variable 3-rotation symmetric functions. This result gave the best known result for the covering radius of the Reed–Muller code $R(1, 9)$. Paper [19] used k-rotation symmetric functions to extend this coding theory work to the Reed–Muller codes with $n = 11$ and 13. More recently, [15] extends the definition of k-rotation symmetric functions to the multi-output case and uses these functions to get new results in the design of cryptographic S-boxes. Also, the 2-rotation symmetric functions are used to construct bent functions in [4].

The 3-symmetric rotation symmetric functions were essential for the coding theory results in [18, 19]. In this paper, we give a detailed theory of the monomial 3-rotation symmetric cubic functions; for brevity, we refer to these functions as (cubic) 3-*functions*. We expect that this theory will be useful in further applications of the 3-rotation symmetric functions. A detailed theory of the monomial 2-rotation symmetric cubic functions was given in [10]. The case $k = 3$ has significant differences, as explained below.

We use the notation 3-$(1, r, s)_{3n}$ (or 3-$(1, r, s)$ when the number of variables is understood) for the cubic 3-function in $3n$ variables generated by the monomial $x_1x_rx_s$. If we assume $r < s \le 3n$ then formula

$$3\text{-}(1, r, s)_{3n} = x_1x_rx_s + x_4x_{r+3}x_{s+3} + \cdots + x_{3n-2}x_{r-3}x_{s-3} \tag{1.1}$$

is called the *standard form* of the above 3-function. We use the notation $(1, r, s)_n$, as in [6], for the (ordinary) cubic MRS function in n variables generated by the monomial $x_1x_rx_s$.

We shall use the notation $[i, j, k]$ for the monomial $x_ix_jx_k$. Unless otherwise specified, all subscripts in given monomials will be taken Mod $3n$ (where the capital Mod notation i Mod $3n$ indicates that i is reduced modulo $3n$ and $i \in \{1, 2, \ldots, 3n\}$) and all 3-functions will have $3n$ variables.

Let $\sigma(f)$ denote a permutation of the variables in the function f. If, given any rotation symmetric (respectively, 3-rotation symmetric) function f, $\sigma(f)$ is also rotation symmetric (respectively, 3-rotation symmetric), we say *σ preserves rotation symmetry* (respectively, *preserves 3-rotation symmetry*). Also, without loss of generality, we assume that if σ : 3-$(1, r, s) \to$ 3-$(1, p, q)$, then $\sigma([1, r, s]) = [1, p, q]$. If $\sigma([1, r, s]) = [i, j, k]$, where $[i, j, k]$ is another monomial term in 3-$(1, p, q)$, then we could take a map β that decreases the index of each variable by $i - 1$ Mod $3n$ and consider instead $\sigma' = \beta \circ \sigma$.

Two Boolean functions f and g in n variables are said to be *affine equivalent* if there exist an invertible matrix A with entries in $\mathbb{F}_2$ and $\mathbf{b} \in \mathbb{V}_n$ such that $f(\mathbf{x}) = g(A\mathbf{x} \oplus \mathbf{b})$. In general, determining whether or not two Boolean functions are affine equivalent is difficult, even in the simplest cases. Recently, however, much work has been done on affine equivalence of MRS functions (see [2, 3, 6–8, 20]). In particular, [20] determines all of the affine equivalence classes for quadratic MRS functions. Also, [6] determines all of the affine equivalence classes under permutations which preserve rotation symmetry for cubic MRS functions, and the recent paper [7] shows that in fact these equivalence classes are the same under all permutations. Also [9] determines all of the affine equivalence classes under permutations which preserve rotation symmetry for the quartic MRS functions.

In this paper we determine the equivalence classes under permutations which preserve 3-rotation symmetry for the cubic 3-functions. Next, using methods similar to those used for ordinary cubic MRS functions in [2], we derive recursions for the weights of the cubic 3-functions. We prove that the roots of the characteristic polynomials (we shall call them *recursion polynomials*) for these recursions have very special forms. This leads to the theorem that the previously determined equivalence classes under permutations are in fact the equivalence classes under arbitrary affine transformations.

2 Some important definitions

For integers, as usual $a|b$ means a divides b.

Definition 2.1 (Form of a monomial). Given a monomial $[a, b, c]$, the *form* of the monomial is defined as the unordered triple $[a \bmod 3,\ b \bmod 3,\ c \bmod 3]$ with entries in $\{0, 1, 2\}$.

It is obvious that if a cubic 3-function is written in the form (1.1), then every monomial in (1.1) has the same form.

Definition 2.2 (Pure, mixed and simple forms). A monomial (or function) whose form is $\{1, 1, 1\}$ is said to be *pure form*. A monomial (or function) whose form has exactly two distinct elements is said to be *mixed form*. A monomial (or function) whose form is has three distinct elements is said to be *simple form*.

A pure form function 3-$(1, r, s)_{3n}$ actually contains only variables x_i with $i \equiv 1 \bmod 3$ subscripts and therefore is essentially the same as the ordinary rotation symmetric function $(1, (r + 2)/3, (s + 2)/3)_n$ with variables $y_i = (x_{3i-2} + 2)/3$, $1 \le i \le n$. Note that by [6, Lemma 3.1, p. 5071], there are $\binom{n-1}{2}/3$ pure form functions if $3 \nmid n$ or $(n^2 - 3n + 6)/6$ pure form functions if $3|n$. A simple form function 3-$(1, r, s)_{3n}$ is a sum of n monomials with each x_i, $1 \le i \le n$, occurring exactly once. There are n choices for each of r and s, so there are n^2 simple form functions. Any two simple form functions are trivially affine equivalent, by a permutation of the variables, to 3-$(1, 2, 3)_{3n}$, which is easy to analyze since all of its monomials have disjoint sets of variables. Hence from now on in this paper we shall only consider the mixed form functions.

Definition 2.3 (Repeated and unique variables). In a mixed form monomial, there are three variables, exactly two of which have indices which are congruent mod 3. We refer to the variables whose indices are congruent mod 3 as *repeated* and the remaining variable as *unique*. The indices of the corresponding variables are called the repeated and unique indices, respectively.

Definition 2.4 (Defining monomial). Given a function 3-$(1, r, s)_{3n}$ with $r < s$ and both r and s are $\not\equiv 1 \bmod 3$, it is clear from (1.1) that x_1 appears in only one monomial. We call $[1, r, s]$ the *defining monomial* of the function. If instead exactly one of r or s is $\equiv 1 \bmod 3$, then x_1 appears in exactly one other monomial, say $[1, t, u]$ with $t < u$. In this case we designate the defining monomial to be the monomial in which $\min(r, t)$ appears.

Definition 2.5 (Form of a function). Given a function 3-$(1, r, s)_{3n}$ with defining monomial $[1, r, s]$, the form of the function is the form of the defining monomial.

The difference between the repeated variables turns out to be essential to the study of equivalences among mixed form 3-functions. Thus, we need the following definition.

Definition 2.6 (χ-value). Let 3-$(1, r, s)$ be a mixed form 3-function with defining monomial $[1, r, s]$. Assume a is the unique index and b, c are repeated (where $a, b, c \in \{1, r, s\}$ and $b < c$). Then we define $\chi = c - b$ to be the *χ-value* for 3-$(1, r, s)$.

Note that since b and c are repeated, χ is always a multiple of 3.

One basic question about cubic MRS 3-functions is how many different mixed form functions there are with $3n$ variables. Our first lemma answers this.

Lemma 2.7. *The number of cubic MRS mixed form 3-functions* 3-$(1, r, s)_{3n}$ *is* $2n^2 - 2n$.

Proof. We begin by counting the number of functions 3-$(1, r, s)_{3n}$ with $r \equiv 1 \bmod 3$ and $s \not\equiv 1 \bmod 3$: we have $n - 1$ choices of r, $2 \le r \le 3n - 1$, and since $r + 1 \le s \le 3n$, we obtain $(2n - 2) + (2n - 4) + (2n - 6) + \cdots + 4 + 2 = n^2 - n$ different 3-functions. The triple $1, r, s$ will not always give the defining monomial for these functions, but the count of them is correct. If both r and s are $\not\equiv 1 \bmod 3$ with $r < s$, then the defining monomials $[1, r, s]$ with $s \not\equiv 1 \bmod 3$ and $r + 1 \le s \le 3n$ for given $r \not\equiv 1 \bmod 3$, $2 \le r \le 3n - 1$, give $(2n - 1) + (2n - 2) + \cdots + 2 + 1 = 2n^2 - n$ different 3-functions. Each monomial is a monomial of form $[1, t, u]$ which appears in some function whose defining monomial $[1, r, s]$

has $r < t$ and is one of the successful candidates. We discard the n^2 simple form functions. Thus the total number of different mixed form functions is $2n^2 - 2n$. □

Example 2.8. For functions 3-$(1, r, s)_9$ ($n = 3$), the 6 defining monomials with exactly one of r or s equivalent to 1 mod 3 are $[1, 2, 4]$, $[1, 2, 7]$, $[1, 3, 4]$, $[1, 3, 7]$, $[1, 4, 8]$, $[1, 4, 9]$. The 15 defining monomials with both $r \not\equiv 1 \bmod 3$ and $s \not\equiv 1 \bmod 3$ are $[1, 2, s]$, $s = 3, 5, 6, 8, 9$; $[1, 3, s]$, $s = 5, 6, 8, 9$; $[1, 5, s]$, $s = 6, 8; 9$; $[1, 6, s]$, $s = 8, 9$; and $[1, 8, 9]$. Note that 9 of these monomials give the simple form functions. The remaining possible monomials containing 1 do not give any new functions; for instance, 3-$(1, 2, 4)_9$ = 3-$(1, 7, 8)_9$, 3-$(1, 2, 7)_9$ = 3-$(1, 4, 5)_9$, etc.

The corresponding count (for example, see [6, Lemma 3.1]) for the ordinary cubic MRS functions $(1, r, s)_n$ is $(n^2 - 3n + 6)/6$ if $3|n$ and $(n^2 - 3n + 2)/6$ otherwise. Thus the count for $n = 9$ is 10. Of course it often happens that a function $(1, a, b)_{3n}$ is equal to the sum of three functions 3-$(1, r, s)_{3n}$, one of which will be 3-$(1, a, b)_{3n}$. For instance, $(1, 2, 3)_9$ = 3-$(1, 2, 3)_9$ + 3-$(1, 2, 9)_9$ + 3-$(1, 8, 9)_9$ and $(1, 2, 6)_9$ = 3-$(1, 2, 6)_9$ + 3-$(1, 5, 6)_9$ + 3-$(1, 5, 9)_9$.

For future reference, we give the linear recursion for the weights of simple form functions in the next lemma. By the remarks after Definition 2.2, it suffices to consider only the functions 3-$(1, 2, 3)_{3n}$.

Lemma 2.9. *Define* $s(n) = \mathrm{wt}(3\text{-}(1, 2, 3)_{3n})$ *for* $n = 1, 2, \ldots$. *Then* $s(1) = 1$, $s(2) = 14$ *and* $s(n)$ *satisfies the linear recursion* $s(n) = 14s(n - 1) - 48s(n - 2)$ *for* $n \geq 2$.

Proof. The function $s(n)$ has n monomials, which have disjoint sets of 3 variables each. Hence [11, Lemma 2.1] can be applied with f = 3-$(1, 2, 3)_{3n}$, $k = 3$ and g = 3-$(1, 2, 3)_{3n}$, so $g_2 = (1, 2, 3)_3$. Since trivially $\mathrm{wt}(s(1)) = 1$, Lemma 2.1 of [11] gives

$$s(n) = 7s(n - 1) + 2^{3n-3} - s(n - 1).$$

This inhomogeneous recursion is easily seen to be equivalent to the homogenous one given in the lemma. □

3 Mixed form functions

In this section we always assume that when we write a mixed form function as 3-$(1, r, s)$, the defining monomial for the function is $[1, r, s]$ (see Definition 2.4).

Lemma 3.1. *Let* 3-$(1, r, s)_{3n}$ *be a mixed form function. For* $a \in \{1, r, s\}$, x_a *is the unique variable if and only if* x_{a+3k} *appears in exactly one monomial of* 3-$(1, r, s)_{3n}$ *for* $k = 0, 1, 2, \ldots, n - 1$. *Similarly* $b, c \in \{1, r, s\}$ *are the repeated variables if and only if each of* $b + 3k$ *and* $c + 3k$ *appear in exactly two monomials for* $k = 0, 1, 2, \ldots, n - 1$.

Proof. Let a, b, c be as above. Since the terms of 3-$(1, r, s)$ are of the form $[1 + 3k, r + 3k, s + 3k]$ and $a \not\equiv b \bmod 3$ and $a \not\equiv c \bmod 3$, it is clear that there do not exist p, q such that $a + 3p = b + 3q$ and $a + 3p = c + 3q$. Now assume x_{a+3k} appears in two monomials. That is, assume there exist p such that $a + 3k \equiv a + 3p \bmod 3n$. This implies $3n|3k - 3p$, but since $k < n$, $k = p$, so x_{a+3k} appears in exactly one monomial.

For the reverse implication, assume x_{a+3k} appears in only one monomial of 3-$(1, r, s)$. This implies that there is no $0 \leq p < n$ such that $a + 3k \equiv b + 3p \bmod 3n$ or $a + 3k \equiv c + 3p \bmod 3n$. Thus $a \not\equiv b \bmod 3n$ and $a \not\equiv c \bmod 3n$, so a is unique.

For the second part of the lemma, assume b, c are repeated and without loss of generality, assume $b < c$. So $\chi = c - b$ by Definition 2.6. We recall that because b, c are repeated, χ is a multiple of three ($3u$). Further, since $c \leq 3n$, $b \geq 1$, and $b \neq c$, we know $0 < \chi < 3n$. Then, in addition to the monomial

$$[a + 3k, b + 3k, c + 3k],$$

x_{b+3k} also appears in the monomial

$$[a + (3k - \chi), b + (3k - \chi), c + (3k - \chi)] = [a + (3k - \chi), b + (3k - \chi), b + 3k]$$

and x_{c+3k} also appears in

$$[a + (3k + \chi), b + (3k + \chi), c + (3k + \chi] = [a + (3k + \chi), c + 3k, c + (3k + \chi)].$$

For the reverse implication, assume x_{b+3k} appears in two monomials:

$$[a+3k, b+3k, c+3k] \quad \text{and} \quad [a+3p, b+3p, c+3p].$$

Since the monomials are distinct, this implies that $b+3k \equiv a+3p \bmod 3n$ (impossible since a is unique) or $b+3k \equiv c+3p \bmod 3n$. Thus $b \equiv c \bmod 3n$ and so b is repeated. □

We now want to examine the relationship between χ and the total number of variables. A helpful tool in this endeavor is the concept of *strings*.

Definition 3.2 (Strings). Given a mixed form function $3\text{-}(a,b,c)_{3n}$ where a is unique and b,c are repeated, let $(3n,\chi) = 3d$ (where χ is as defined above) and $3n = 3dl$. We define the *i-th string* of $3\text{-}(a,b,c)$ to be the set of monomials $\mathcal{S}_i$ such that

$$\mathcal{S}_i = \{[a+3i+v\chi, b+3i+v\chi, c+3i+v\chi] : v = 0,1,\ldots,l-1\},$$

where $i = 0,1,\ldots,d-1$.

Example 3.3. Consider the function $f = 3\text{-}(1,2,7)_{15}$. The repeated variables in the defining monomial of f are x_1 and x_7. The unique variable is x_2. Thus, we have that the χ-value of f is $7-1=6$, $(3n,\chi) = (15,6) = 3$ and $3n = 3\cdot 5 = 15 = 3dl = 3\cdot 1\cdot l$, so comparing with Definition 3.2 we have $3d = 3$ and $l = 5$. Thus, we have one string of length 5. It is

$$\mathcal{S}_0 = \{[1,2,7],[7,8,13],[13,14,4],[4,5,10],[10,11,1]\}.$$

Lemma 3.4. *Every monomial of the mixed form function* $3\text{-}(1,r,s)$ *is in one and only one string.*

Proof. Let $3\text{-}(a,b,c)_{3n}$ be a mixed form function such that a is unique and b,c are repeated. It is clear that each monomial appears in at least one string, so we begin by showing that no monomial appears in more than one string. Assume that a given monomial $[p,q,w]$ appears in $\mathcal{S}_i$ and $\mathcal{S}_j$. This implies that there exist k_i, k_j such that

$$[p,q,w] = [a+3i+k_i\chi, b+3i+k_i\chi, c+3i+k_i\chi],$$
$$[p,q,w] = [a+3j+k_j\chi, b+3j+k_j\chi, c+3j+k_j\chi]$$

and thus

$$[a+3i+k_i\chi, b+3i+k_i\chi, c+3i+k_i\chi] = [a+3j+k_j\chi, b+3j+k_j\chi, c+3j+k_j\chi].$$

Since, by Lemma 3.1, each of the unique terms appears in only one monomial, we must have that

$$a+3i+k_i\chi \equiv a+3j+k_j\chi \bmod 3n.$$

This implies that $3i+k_i\chi \equiv 3j+k_j\chi \bmod 3n$, so $3n|3i-3j+(k_i-k_j)\chi$. Since $3d|3n$ and $3d|\chi$, $3d$ must divide $3(i-j)$. But, since $i,j \le d-1$, we have $i=j$, as required. Now, since χ is $3u$, it is easy to see that there is no pair i,k_i such that $a = b+3i+k_i\chi$. Further, we claim that within a given string, there is no pair k_i,k_j such that $a+3i+k_i\chi = a+3i+k_j\chi$. If there is, then we have $k_i\chi \equiv k_j\chi \bmod 3n$, which would imply $3n|(k_i-k_j)\chi$. Since $\gcd(3n,\chi) = 3d$ and $3dl = 3n$, we must have $l|(k_i-k_j)$. Since $k_i,k_j \le l-1$, this implies $k_i = k_j$.

Thus, in each string there are l unique monomials, which do not appear in any other string. As a result, we have accounted for l monomials in each of the d strings, or $ld = n$ total monomials. Since every 3-function in $3n$ variables is composed of n monomials, we have the desired result. □

Apart from being useful in identifying specific monomials, the presence of unique variables limits the ways in which we can permute the indices of 3-functions to find affine equivalent ones. In particular, we have the following lemma.

Lemma 3.5. *If f is a mixed form function and a permutation $\sigma : f \to g$ preserves 3-rotation symmetry, then g must be mixed form.*

Proof. Let 3-$(1, r, s)$ be a mixed form function and assume $\sigma : f \to g$ preserves 3-rotation symmetry. Let $a \in \{1, r, s\}$ be unique and b, c be repeated. If

$$3\text{-}f_{r,s} = x_a x_b x_c + x_{a+3} x_{b+3} x_{c+3} + \cdots + x_{a-3} x_{b-3} x_{c-3},$$

then

$$g = \sigma(f) = x_{\sigma(a)} x_{\sigma(b)} x_{\sigma(c)} + x_{\sigma(a+3)} x_{\sigma(b+3)} x_{\sigma(c+3)} + \cdots + x_{\sigma(a-3)} x_{\sigma(b-3)} x_{\sigma(c-3)}.$$

By Lemma 3.1, for each $k = 0, 1, 2, \ldots, n-1$, we know that x_{a+3k} appears in exactly one monomial and x_{b+3k} and x_{c+3k} each appear in two. Thus $x_{\sigma(a+3k)}$ must appear in exactly one monomial of g and $x_{\sigma(b+3k)}$, $x_{\sigma(c+3k)}$ must each appear in two. Thus each monomial of g contains 1 unique variable and 2 repeated ones and so g is mixed form. □

Remark 3.6. We note that the above lemma does not imply that f and g have the *same* form (recall Definition 2.5), only that they are both mixed form functions. As we shall see later, the equivalence classes are determined by the distance between the repeated variables (the χ-value), not by a shared form.

With the previous lemma, we have shown that mixed form functions can only be affine equivalent to other mixed form functions. In addition, during the proof of said lemma, we indicated that a 3-rotation symmetry preserving mapping between mixed functions must send unique variables to unique variables and repeated variables to repeated variables. Further, since the repeated variables each appear in two different monomials, if we know the image of a repeated variable under a 3-rotation symmetry preserving map σ, we can get some information about the image of both the monomials in which it appears. We use these ideas in the proof of Theorem 3.8 below, which gives a simple way to define the equivalence classes for functions 3-$(1, r, s)_{3n}$ under permutations which preserve 3-rotation symmetry. We shall need the following useful lemma for the proof.

Lemma 3.7. *If σ : 3-$(1, r, s) \to$ 3-$(1, p, q)$ preserves 3-rotation symmetry and has the property that $\sigma(t) = u$ implies $\sigma(t + k\chi) = u + k\chi'$ for all $k = 0, 1, \ldots, 3n-1$ (where χ and χ' are the χ-values for 3-$(1, r, s)$ and 3-$(1, p, q)$, respectively), then $(3n, \chi) = (3n, \chi')$.*

Proof. Let σ be as above. Let $(3n, \chi) = 3d$ and $(3n, \chi') = 3d'$. Let l and μ satisfy $3dl = 3n$ and $3d\mu = \chi$ and l' and μ' satisfy $3d'l' = 3n$ and $3d'\mu' = \chi'$. If $\sigma(t) = u$, then

$$u = \sigma(t + 3dl\mu) = \sigma(t + l\chi) = u + l\chi'.$$

Thus $u \equiv u + l\chi'$ Mod $3n$ and so $3d | \chi'$. Since $3d$ also divides $3n$, this implies $3d | 3d'$. Since σ is a permutation of variables, there exists a reverse permutation σ^{-1} : 3-$(1, p, q) \to$ 3-$(1, r, s)$ which preserves 3-rotation symmetry and has the property that $\sigma^{-1}(u) = t$ implies $\sigma^{-1}(u + l\chi') = t + l\chi$. Using the same argument as above, we have that $3d' | \chi$. Again, since $3d'$ also divides $3n$, this implies $3d' | 3d$. Thus $3d = 3d'$, as required. □

Theorem 3.8. *Let $f =$ 3-$(1, r, s)_{3n}$ and $g =$ 3-$(1, p, q)_{3n}$ be mixed form functions which have associated χ-values χ_f and χ_g. Then there exists a permutation $\sigma : f \to g$ which preserves 3-rotation symmetry if and only if* $\gcd(3n, \chi_f) = \gcd(3n, \chi_g)$.

Proof. We begin with the forward implication. Let $f =$ 3-(a, b, c) and $g =$ 3-(w, p, q). Suppose a, w are the unique variables of f and g, respectively, and $\chi_f = c - b = 3m$ and $\chi_g = q - p = 3m'$. Assume $\sigma : f \to g$ preserves 3-rotation symmetry.

From the proof of Lemma 3.5, we know that σ maps the unique variables in f to the unique variables in g. Thus, given any monomial $[a + 3k, b + 3k, c + 3k]$ in f, we have

$$\begin{aligned} \sigma\big([a + 3k, b + 3k, c + 3k]\big) &= [\sigma(a + 3k), \sigma(b + 3k), \sigma(c + 3k)] \\ &= [w + 3\beta, \sigma(b + 3k), \sigma(c + 3k)] \\ &= [w + 3\beta, p + 3\beta, q + 3\beta], \end{aligned} \tag{3.1}$$

where the last equality results from the fact that the unique variable with index $w + 3\beta$ occurs only in one monomial.

Case 1: Assume $3m \not\equiv -3m \bmod 3n$. Since b, c are repeated, x_{b+3k} also appears in the monomial

$$[a+3k-3m, b+3k-3m, c+3k-3m] = [a+3(k-m), b+3(k-m), b+3k]$$

and x_{c+3k} also appears in the monomial

$$[a+3k+3m, b+3k+3m, c+3k+3m] = [a+3(k+m), c+3k, c+3(k+m)].$$

Since $b \neq c$, $3m \neq 0$ and by assumption $3m \not\equiv -3m$, we have

$$a+3k \neq a+3(k+m) \neq a+3(k-m).$$

Thus the three monomials

$$[a+3k, b+3k, c+3k], \quad [a+3(k-m), b+3(k-m), b+3k], \quad [a+3(k+m), c+3k, c+3(k+m)]$$

are different, and hence their images under σ must be different. From (3.1), we know

$$\sigma([a+3k, b+3k, c+3k]) = [w+3\beta, p+3\beta, q+3\beta]. \tag{3.2}$$

Thus,

$$\sigma([a+3(k-m), b+3(k-m), b+3k]) = [\sigma(a+3(k-m)), \sigma(b+3(k-m)), p+3\beta].$$

But, by Lemmas 3.1 and 3.4, σ must send $x_{a+3(k-m)}$ to a variable with index of the form $w+3\alpha_1$, which appears uniquely in the monomial $[w+3\alpha_1, p+3\alpha_1, q+3\alpha_1]$. So we have

$$[\sigma(a+3(k-m)), \sigma(b+3(k-m)), p+3\beta] = [w+3\alpha_1, p+3\alpha_1, q+3\alpha_1]. \tag{3.3}$$

Since $a+3k \neq a+3(k-m)$, we have $w+3\alpha_1 = \sigma(a+3(k-m)) \neq \sigma(a+3k) = w+3\beta$. So $p+3\alpha_1 \neq p+3\beta$. Thus, we have $q+3\alpha_1 = p+3\beta$ which implies $3\alpha_1 = -(q-p)+3\beta = -\chi_g + 3\beta$.

Similarly,

$$\begin{aligned}\sigma([a+3(k+m), c+3k, c+3(k+m)]) &= [\sigma(a+3(k+m)), q+3\beta, \sigma(c+3(k+m))] \\ &= [w+3\alpha_2, p+3\alpha_2, q+3\alpha_2].\end{aligned} \tag{3.4}$$

From above, none of $a+3(k+m)$, $c+3k$, $c+3(k+m)$ is equal to $a+3k$, so we have

$$p+3\alpha_2 = q+3\beta \quad \text{or} \quad 3\alpha_2 = (q-p)+3\beta = \chi_g + 3\beta.$$

From (3.2), (3.3), (3.4) we have that, if (3.2) is true for some β, $0 \leq \beta \leq n-1$, then

$$\sigma([a+3k \pm \chi_f, b+3k \pm \chi_f, c+3k \pm \chi_f]) = [w+3\beta \pm \chi_g, p+3\beta \pm \chi_g, q+3\beta \pm \chi_g].$$

Since every variable of $f = (1, r, s)_{3n}$ can be represented by $i+3k$, where $i \in \{a, b, c\}$, $k = 0, 1, \ldots, n-1$, so σ satisfies

$$\sigma(t) = \tau \implies \sigma(t \pm \chi_f) = \tau \pm \chi_g.$$

Thus from Lemma 3.7, we have the desired result, namely, $(3n, \chi_f) = (3n, \chi_g)$.

Case 2: If $3m \equiv -3m \bmod 3n$, then $3m = n$. Since each of the two repeated terms appears in two distinct monomials (which in this case happen to be the *same* two monomials), then for every $k = 0, 1, \ldots, n-1$, we still have two distinct monomials which differ in their unique term:

$$[a+3k, b+3k, c+3k] \quad \text{and} \quad [a+3m+3k, b+3k+3m, c+3k+3m] = [a+3m+3k, c+3k, b+3k].$$

Applying σ to each of these monomials gives us (3.2) in the first case and

$$\sigma([a+3k+3m, c+3k, b+3k]) = [w+3\alpha, p+3\alpha, q+3\alpha] = [w+3\alpha, q+3\beta, p+3\beta]$$

in the second. Since $m \not\equiv 0$, we must have $p + 3\alpha \equiv q + 3\beta$ and $q + 3\alpha \equiv p + 3\beta$. Thus $3\alpha \equiv (q - p) + 3\beta$ and $3\alpha \equiv -(q - p) + 3\beta$. So $3m' = (q - p) \equiv -(q - p) = -3m' \bmod 3n$. Hence, $3m' \equiv -3m' \bmod 3n$ so $3m' = n = 3m$ and $\gcd(3n, \chi_f) = \gcd(3n, \chi_g)$ trivially.

For the reverse direction, we assume that $(3n, \chi_f) = (3n, \chi_g) = 3d$, then we define $\sigma : f \to g$ as follows:

$$\sigma(a + 3i + k\chi_f) = w + 3i + k\chi_g,$$
$$\sigma(b + 3i + k\chi_f) = p + 3i + k\chi_g,$$
$$\sigma(c + 3i + k\chi_f) = q + 3i + k\chi_g.$$

We can see that this map is one-to-one, since given monomials $[a + 3i + k_i\chi_f, b + 3i + k_i\chi_f, c + 3i + k_i\chi_f]$ and $[a + 3j + k_j\chi_f, b + 3j + k_j\chi_f, c + 3j + k_j\chi_f]$ such that

$$\sigma([a + 3i + k_i\chi_f, b + 3i + k_i\chi_f, c + 3i + k_i\chi_f]) = \sigma([a + 3j + k_j\chi_f, b + 3j + k_j\chi_f, c + 3j + k_j\chi_f])$$

by the definition of σ, we have

$$\sigma([a + 3i + k_i\chi_f, b + 3i + k_i\chi_f, c + 3i + k_i\chi_f]) = [w + 3i + k_i\chi_g, p + 3i + k_i\chi_g, q + 3i + k_i\chi_g]$$

and

$$\sigma([a + 3j + k_j\chi_f, b + 3j + k_j\chi_f, c + 3j + k_j\chi_f]) = [w + 3j + k_j\chi_g, p + 3j + k_j\chi_g, q + 3j + k_j\chi_g]$$

which implies

$$[w + 3i + k_i\chi_g, p + 3i + k_i\chi_g, q + 3i + k_i\chi_g] = [w + 3j + k_j\chi_g, p + 3j + k_j\chi_g, q + 3j + k_j\chi_g].$$

Since w is unique, this implies

$$w + 3i + k_i\chi_g = w + 3j + k_j\chi_g.$$

So $3n | 3(i - j) + (k_i - k_j)\chi_g$. Since $3d | 3n$ and $3d | \chi_g$, we have $3d | 3(i - j)$. But, since $i, j < d$, we have $i = j$ and $k_i = k_j$. In addition, since there are the same number of monomial terms in f as in g, σ must map f onto g. Since both f and g are 3-rotation symmetric, σ preserves 3-rotation symmetry, as required. □

Corollary 3.9. *Two 3-functions in $3n$ variables whose defining monomials are given by $[1, r, s]$ and $[1, p, q]$ are affine equivalent by some permutation for* all *n if and only if their χ-values are equal.*

Proof. Rotation symmetric functions are affine equivalent if there exists a permutation of variables that maps one to the other. By Theorem 3.8, the existence of such a mapping between two functions f and g is equivalent to $\gcd(3n, \chi_f) = \gcd(3n, \chi_g)$. In order for this equivalence to hold for all n, we must have $\chi_f = \chi_g$. □

In light of Corollary 3.9, we see that every 3-function in $3n$ variables shares many of its properties with every other 3-function in $3n$ variables with the same χ-value (since they are all affine equivalent). As a result, we will often refer to these functions simply by $f_{3n,\chi}$ (or f_χ if the number of variables is clear), where the particular member of the equivalence class being discussed is not important.

Theorem 3.8 enables us to give a simple formula for the number of equivalence classes under permutations which preserve 3-rotation symmetry. To state this, we need the number theory function $\tau(n)$ = the number of positive integer divisors (including 1 and n) of the integer n.

Lemma 3.10. *For any given number of variables $3n$, the number of equivalence classes under permutations which preserve 3-rotation symmetry for the functions 3-$(1, r, s)_{3n}$ is $\tau(n) - 1$.*

Proof. By Theorem 3.8, two 3-functions are equivalent under some permutation which preserves 3-rotation symmetry if and only if the functions have the same value of $\gcd(3n, \chi) = 3\gcd(n, \chi/3)$, so there is one equivalence class for each possible value of the gcd. Since χ is $3u$ and must be $\le 3n - 3$, this gives $\tau(n) - 1$ classes. □

We remark that the count of equivalence classes in Lemma 3.10 is very small (because of the well-known result that $\tau(n) = O(n^\epsilon)$ for any $\epsilon > 0$) compared to the number of equivalence classes for ordinary RS functions $(1, r, s)$ in n variables. The latter count is $> cn$ and the constant c depends heavily on r and s (see [3, 6]); also, there is no simple formula for the number of those classes (see [3]).

	$s=3$	$s=4$	$s=5$	$s=6$	$s=7$	$s=8$	$s=9$	$s=10$
$r=2$	2	3	3	2	5	5	2	9
$r=3$		3	2	3	5	2	5	9
$r=4$			3	3	4	3	3	6
$r=5$				2	5	3	2	9
$r=6$					5	2	3	9
$r=7$						5	5	6
$r=8$							2	9
$r=9$								9

Table 1. Recursion order for 3-$f_{r,s}$.

4 Recursions for weights of cubic 3-functions

Using the methods in [1, 2] we can prove that for any 3-function 3-$(1,r,s)$ with $1<r<s$ the sequence of weights $\{\mathrm{wt}(3\text{-}(1,r,s)_{3n}) : 3n \geq s\}$ satisfies a linear recursion with integer coefficients. In fact, unlike the case of the ordinary RS functions analyzed in [1], the order (order = degree of recursion polynomial) of the recursion for mixed form functions depends only on the χ-value for 3-$(1,r,s)$ (recall Definition 2.6), rather than on r and s. In fact, if $q=\chi/3$ then the order of the recursion for the mixed form functions is q^2-q+3 (see Theorem 6.4 below). The recursion orders are given in Table 1, which includes pure and simple form functions for completeness. We use the abbreviated notation 3-$f_{r,s}$ for 3-$(1,r,s)$.

In Table 1, each recursion of order i is identical to all the other recursions of order i. For instance, the recursion for 3-$f_{2,4}$ is identical to the recursions for 3-$f_{2,5}$, 3-$f_{3,4}$, 3-$f_{4,5}$, and each of the other (r,s) pairs in the table with recursion order 3. This confirms the results found in Section 3, since 3-$f_{2,4}$, 3-$f_{2,5}$, 3-$f_{3,4}$, and 3-$f_{4,5}$ are all mixed form functions with $\chi=3$ (see Corollary 3.9).

We postpone discussing the proof that the above recursions exist, because in Section 5 below we show that a relatively simple direct proof, not using the methods in [1, 2], can be given. The details are in Theorem 6.4.

Let the recursion polynomial for the weights of a mixed form function with given χ be $F_\chi(x)$. Then Table 2 lists $\chi : F_\chi(x)$ for $3 \leq \chi \leq 18$. Let $d(\chi)=\deg(F_\chi(x))-1$. It is easy to see that 8 is a root of every $F_\chi(x)$; let the remaining roots be $\{\alpha_{j,\chi} : 1 \leq j \leq d(\chi)\}$. Define

$$W_{n,\chi} = \sum_{i=0}^{2^{3n}-1} (-1)^{f(\mathbf{v}_i)} = 2^{3n} - 2\,\mathrm{wt}(f), \tag{4.1}$$

where f is any 3-function in $3n$ variables with the given χ value. We call $W_{n,\chi}$ the *Walsh value* for f. See [12, pp. 7–9] for more general functions, called Walsh transforms, related to (4.1). It follows from Theorem 3.8 that for given n, $W_{n,\chi}$ depends only on χ and not on the choice of the 3-function f. It follows from the basic theory of recursions (for example, [13, pp. 1–3]) that

$$W_{n,\chi} = \sum_{j=1}^{d(\chi)} c_{j,\chi}\alpha_{j,\chi}^n \tag{4.2}$$

for some complex numbers $c_{j,\chi}$. Theorem 6.4 gives explicit values for all of the $\alpha_{j,\chi}$.

5 Weights and equivalence classes

It is well known that for any Boolean function f, $\mathrm{wt}(f)$ is invariant under affine transformations. For cubic RS functions, it is possible for two functions with the same weight to be in different equivalence classes under permutations which preserve rotation symmetry; the case of cubic RS functions in 8 variables already

	$F_\chi(x)$
$\chi = 3$	$x^3 - 12x^2 + 16x + 128$
$\chi = 6$	$x^5 - 12x^4 + 32x^3 - 64x^2 + 256x + 2048$
$\chi = 9$	$x^9 - 12x^8 + 16x^7 + 192x^6 - 768x^5 + 1024x^4 + 4096x^3 + 49152x^2 - 65536x - 524288$
$\chi = 12$	$x^{15} - 12x^{14} + 16x^{13} + 128x^{12} + 512x^{11} - 6144x^{10} + 8192x^9 + 65536x^8 - 131072x^7 + 1572864x^6$ $-2097152x^5 - 16777216x^4 - 16777216x^3 + 201326592x^2 - 268435456x - 2147483648$
$\chi = 15$	$x^{23} - 12x^{22} + 16x^{21} + 128x^{20} + 3072x^{18} - 36864x^{17} + 49152x^{16} + 393216x^{15} - 6291456x^{13} + 75497472x^{12}$ $-100663296x^{11} - 805306368x^{10} - 3221225472x^8 + 38654705664x^7 - 51539607552x^6 - 412316860416x^5$ $+1099511627776x^3 - 13194139533312x^2 + 17592186044416x + 140737488355328$
$\chi = 18$	$x^{33} - 12x^{32} + 16x^{31} + 128x^{30} + 20480x^{27} - 245760x^{26} + 327680x^{25} + 2621440x^{24} - 251658240x^{21}$ $+3019898880x^{20} - 4026531840x^{19} - 32212254720x^{18} - 1030792151040x^{15} + 12369505812480x^{14}$ $-16492674416640x^{13} - 131941395333120x^{12} + 1407374883553280x^9 - 16888498602639360x^8$ $+22517998136852480x^7 + 180143985094819840x^6 + 1152921504606846976x^3$ $-1383505805528216371 2x^2 + 1844674407370955161 6x + 1475739525896764 1928$

Table 2. List of $\chi : F_\chi(x)$.

gives an example [6, Remark 3.10, p. 5075]. The next theorem shows that such examples are impossible for cubic 3-functions. Since the equivalence classes for cubic 3-functions under permutations which preserve 3-rotation symmetry are very large (see the remarks in the paragraph after the proof of Lemma 3.10), it is plausible that they cannot be made any larger by applying all of the affine transformations. Theorem 5.1 proves this is true. A similar result for the equivalence classes for ordinary cubic RS functions (these classes were determined in [6]) was conjectured in [6, Remark 3.9, p. 5075], but, since these equivalence classes are so much smaller and distinct classes can have functions with the same weight, the proof may be difficult.

Theorem 5.1. *Let $C(3n)$ denote the number of equivalence classes for mixed form functions 3-$(1, r, s)_{3n}$ under permutations which preserve 3-rotation symmetry. Let $w_1, \ldots, w_{C(3n)}$ denote the list of weights of representative functions for the classes. Then these $C(3n)$ weights are all different. Thus the equivalence classes in Lemma 3.10 are the same as the equivalence classes under all affine transformations.*

Before we prove Theorem 5.1, we need the following results (recall the notation $f_{3n,\chi}$ introduced after Corollary 3.9).

Theorem 5.2. *Given a 3-function $f_{3n,\chi}$ such that* $\gcd(n, \chi/3) = d$ *and $l = n/d$, then*

$$\mathrm{wt}(f_{3n,\chi}) = \frac{1}{2}\left(2^{3n} - \left(2^{3l} - 2\,\mathrm{wt}(h_{3l,3})\right)^d\right),$$

where $h_{3l,3} = 3\text{-}(1, 2, 4)_{3l}$.

Theorem 5.2 is an analog of [11, Theorem 2.2]. Before we prove Theorem 5.2, we will need the following well-known lemma [11, Lemma 2.1].

Lemma 5.3. *Suppose f can be decomposed as $g + h$ where the variables of g and h are disjoint. (Without loss of generality assume g uses variables $x_1, \ldots, x_k$ and h uses variables $x_{k+1}, \ldots, x_n$). Then*

$$\mathrm{wt}(f) = \mathrm{wt}(g + h) = \mathrm{wt}(g)(2^{n-k} - \mathrm{wt}(h)) + (2^k - \mathrm{wt}(g))\,\mathrm{wt}(h).$$

Proof of Theorem 5.2. By Corollary 3.9, all 3-functions in $3n$ variables with the same χ-value are affine equivalent. Therefore, since weight is affine-invariant, it suffices to consider only $f_\chi = 3\text{-}(1, 2, \chi + 1)_{3n}$. Recall from Definition 3.2 that the i-th string of f_χ is defined to be the set of monomials $\mathscr{S}_i$ such that

$$\mathscr{S}_i = \{[1 + 3i + v\chi, 2 + 3i + v\chi, \chi + 1 + 3i + v\chi] : v = 0, 1, \ldots, l - 1\},$$

where $i = 0, 1, \ldots, d - 1$. Note that, from this definition, the length of each string is l and there are d strings. By Lemma 3.4, the sets of monomials that make up the d strings are disjoint. By definition, each string contains exactly $3l$ monomials, so by relabeling the variables of f_χ, we can view f_χ as the sum of d disjoint copies

of $h_{3l,3}$. This can be done as follows: Let the i-th string of f_χ be given by

$$\{[1+3i, 2+3i, 1+3i+\chi], [1+3i+\chi, 2+3i+\chi, 1+3i+2\chi], \ldots, [1+3i-\chi, 2+3i-\chi, 1+3i]\}.$$

This string can be mapped to

$$\{[3li+1, 3li+2, 3li+4], [3li+4, 3li+5, 3li+7], \ldots, [3li-2, 3li+3l, 3li+1]\}. \tag{5.1}$$

The above can easily been seen to be affine equivalent to $h_{3l,3}$. Since each of the d strings of f_χ can be mapped to one similar to (5.1), we can see that f is affine equivalent to d copies of $h_{3l,3}$. Since weight is affine invariant, we have

$$\mathrm{wt}(f_\chi) = \mathrm{wt}\Big(\sum_{i=1}^{d} h_{3l,3,i}\Big), \tag{5.2}$$

where $h_{3l,3,i}$ is the i-th copy of $h_{3l,3}$ whose defining monomial is $[3li+1, 3li+2, 3li+4]$. Using Lemma 5.3, it is easy to see that

$$\mathrm{wt}(f_\chi) = \mathrm{wt}\Big(\sum_{i=1}^{d} h_{3l,3,i}\Big) = \mathrm{wt}(h_{3l,3,1})\Big(2^{3n-3l} - \mathrm{wt}\Big(\sum_{i=1}^{d-1} h_{3l,3,i}\Big)\Big) + (2^{3l} - \mathrm{wt}(h_{3l,3,1}))\,\mathrm{wt}\Big(\sum_{i=1}^{d-1} h_{3l,3,i}\Big).$$

Since $\mathrm{wt}(h_{3l,3,i})$ is the same for all i, we can write $\mathrm{wt}(h_{3l,3})$ (without the index) whenever we are computing the weight of a single copy of $h_{3l,3}$. Using this notation and expanding (5.2) further, we get

$$\mathrm{wt}\Big(\sum_{i=1}^{m} h_{3l,3,i}\Big) = (2^{3l} - \mathrm{wt}(h))\,\mathrm{wt}\Big(\sum_{i=1}^{m-1} h_{3l,3,i}\Big) + \mathrm{wt}(h_{3l,3})\,\mathrm{wt}\Big(2^{3n-3ml} - \sum_{i=1}^{m-1} h_{3l,3,i}\Big)$$

which can be solved (see [11, Theorem 2.2]) to give

$$\mathrm{wt}(f_{3n,\chi}) = \mathrm{wt}\Big(\sum_{i=1}^{d} h_{3l,3,i}\Big) = \frac{1}{2}\big(2^{3n} - (2^{3l} - 2\,\mathrm{wt}(h_{3l,3}))^d\big)$$

as required. □

Corollary 5.4. *With d and l as defined above, we have*

$$\mathrm{wt}(f_{3n,\chi}) = \frac{1}{2}\big(2^{3n} - ((2(1+\sqrt{5}))^l + (2(1-\sqrt{5}))^l)^d\big).$$

Proof. From Theorem 5.2, we have

$$\mathrm{wt}(f_{3n,\chi}) = \frac{1}{2}\big(2^{3n} - (2^{3l} - 2\,\mathrm{wt}(h_{3l,3}))^d\big). \tag{5.3}$$

If we let $\alpha_1, \alpha_2, \alpha_3$ be the roots of the recursion polynomial for $\chi = 3$, by the remarks surrounding (4.2) there exist c_1, c_2, c_3 such that, for any n,

$$\mathrm{wt}(f_{3n,3}) = \sum_{i=1}^{3} c_i \alpha_i^n.$$

After solving for the α_i's and their associated c_i's, we can see that $\alpha_1 = 8$, $\alpha_2 = 2(1+\sqrt{5})$, $\alpha_3 = 2(1-\sqrt{5})$ and $c_1 = 1/2$, $c_2 = c_3 = -1/2$. Thus we can rewrite (5.3) as

$$\begin{aligned}
\mathrm{wt}(f_{3n,\chi}) &= \frac{1}{2}\Big(2^{3n} - \Big(2^{3l} - 2\Big(\frac{1}{2}\big(8^l - (2(1+\sqrt{5}))^l - (2(1-\sqrt{5}))^l\big)\Big)\Big)^d\Big) \\
&= \frac{1}{2}\Big(2^{3n} - \big(8^l - (8^l - (2(1+\sqrt{5}))^l - (2(1-\sqrt{5}))^l)\big)^d\Big) \\
&= \frac{1}{2}\Big(2^{3n} - \big((2(1+\sqrt{5}))^l + (2(1-\sqrt{5}))^l\big)^d\Big)
\end{aligned}$$

as required. □

We can now use the above results to prove Theorem 5.1.

Proof of Theorem 5.1. To prove Theorem 5.1 we need only prove that for a fixed n, every divisor d of n gives rise to a unique weight. That is, we need to prove that

$$\frac{1}{2}\big(2^{3n} - (2^{3n/d} - 2\,\mathrm{wt}(h_{3n/d,3}))^d\big)$$

is unique for all d that divide n. Let $d_1 \le d_2$ such that $d_i | n$ for $i = 1, 2$. Let $f_{3n,3d_1}$ and $f_{3n,3d_2}$ be 3-functions in $3n$ variables with $\chi_i = 3d_i$. Assume $\mathrm{wt}(f_{3n,3d_1}) = \mathrm{wt}(f_{3n,3d_2})$. We will show that $d_1 = d_2$. By Theorem 5.2, since the weights of the functions f_{3n,χ_i} are equal, we have

$$\frac{1}{2}\big(2^{3n} - (2^{3n/d_1} - 2\,\mathrm{wt}(h_{3n/d_1,3}))^{d_1}\big) = \frac{1}{2}\big(2^{3n} - (2^{3n/d_2} - 2\,\mathrm{wt}(h_{3n/d_2,3}))^{d_2}\big)$$

which implies

$$(2^{3n/d_1} - 2\,\mathrm{wt}(h_{3n/d_1,3}))^{d_1} = (2^{3n/d_2} - 2\,\mathrm{wt}(h_{3n/d_2,3}))^{d_2}.$$

Using Corollary 5.4, we can rewrite the above as

$$\big((2(1+\sqrt{5}))^{n/d_1} + (2(1-\sqrt{5}))^{n/d_1}\big)^{d_1} = \big((2(1+\sqrt{5}))^{n/d_2} + (2(1-\sqrt{5}))^{n/d_2}\big)^{d_2}. \tag{5.4}$$

We can see that the above can only hold if $d_1 = d_2$ as follows. Since

$$(1+x)^a = \sum_{i=0}^{a} \binom{a}{i} x^i,$$

plugging in $\sqrt{5}$ and $-\sqrt{5}$ for x gives

$$(1+\sqrt{5})^a = \sum_{i=0}^{a} \binom{a}{i} 5^{i/2} \tag{5.5}$$

and

$$(1-\sqrt{5})^a = \sum_{i=0}^{a} \binom{a}{i} (-1)^i 5^{i/2}, \tag{5.6}$$

respectively. By adding (5.5) to (5.6) we see that

$$(1+\sqrt{5})^a + (1-\sqrt{5})^a = 2\sum_{i=0}^{a/2} \binom{a}{2i} 5^i$$

if a is even, and

$$(1+\sqrt{5})^a + (1-\sqrt{5})^a = 2\sum_{i=0}^{(a-1)/2} \binom{a}{2i} 5^i$$

if a is odd. Now, for $i = 1, 2$, let

$$t_i = \begin{cases} n/d_i & \text{if } n/d_i \text{ is even,} \\ n/d_i - 1 & \text{otherwise.} \end{cases}$$

Thus (5.4) is equal to

$$\Big(4\sum_{i=0}^{t_1/2} \binom{n/d_1}{2i} 5^i\Big)^{d_1} = \Big(4\sum_{i=0}^{t_2/2} \binom{n/d_2}{2i} 5^i\Big)^{d_2}$$

or

$$4^{d_1}\Big(\sum_{i=0}^{t_1/2} \binom{n/d_1}{2i} 5^i\Big)^{d_1} = 4^{d_2}\Big(\sum_{i=0}^{t_2/2} \binom{n/d_2}{2i} 5^i\Big)^{d_2}$$

and so

$$\Big(\sum_{i=0}^{t_1/2} \binom{n/d_1}{2i} 5^i\Big)^{d_1} = 4^{d_2-d_1}\Big(\sum_{i=0}^{t_2/2} \binom{n/d_2}{2i} 5^i\Big)^{d_2}.$$

By looking at each side modulo 5, only the terms with $i = 0$ remain, and so equality can only hold if $d_1 = d_2$, as required. □

6 Recursion orders and crucial weights

We can now prove some results on the recursion orders for the different values of χ. Notice that, for any $\chi = 3q$, if $3n \neq 3qk = k\chi$, then $\gcd(n, q) \neq q$. So by Theorem 3.8, there exists a χ' dividing χ such that $\mathrm{wt}(f_{3n,\chi}) = \mathrm{wt}(f_{3n,\chi'})$. This means that $f_{3n,\chi}$ "inherits" its weight from a function with a smaller χ-value for all $3n$ other than those that are multiples of χ. Since $f_{3n,\chi}$ is distinguished from functions with smaller χ values by its behavior at these values of $3n$, it is of interest to study $\mathrm{wt}(f_{k\chi,\chi})$ at these values. We begin with the following definition.

Definition 6.1 (Crucial weights and values). Consider a fixed χ. We define the *crucial weights* (resp. *crucial (Walsh) values*) for χ to be the sequence of weights $\mathrm{wt}(f_{k\chi,\chi})$, $k = 2, 3, \ldots$ (respectively, sequence of Walsh values $W_{k\chi/3,\chi}$, $k = 2, 3, \ldots$), where $f_{3n,\chi} = 3\text{-}(1, 2, \chi + 1)_{3n}$.

By Theorem 3.8, all 3-functions with the same χ-value are affine equivalent and since weight is affine invariant, we only need to mention the particular function $3\text{-}(1, 2, \chi + 1)_{3n}$ in Definition 6.1. The above work is summarized in the next lemma.

Lemma 6.2. *For any χ-value, in order to determine the sequence of Walsh values*

$$Wv(\chi) = \{W_{n,\chi} : n = 2, 3, \ldots\}$$

(for the function $3\text{-}(1, 2, \chi + 1)$ and so for any 3-function with the same χ-value), it suffices to know the sequence of crucial Walsh values

$$Cv(\chi) = \{W_{k\chi/3,\chi} : k = 2, 3, \ldots\}$$

and the sequences $Wv(\chi')$ for all $\chi' < \chi$ such that χ' divides χ. Thus all of the sequences $Wv(\chi)$, $\chi = 3, 4, \ldots$ can be determined successively by finding $Wv(3)$ and then the successive sequences of crucial values $Cv(\chi)$, $\chi = 4, 6, \ldots$.

The next lemma gives a recursion for the crucial weights (recall equation (4.1) which gives the relation between weights and Walsh values).

Lemma 6.3. *For $\chi = 3q$, the crucial weights for χ satisfy the recursion of order $q + 2$, whose polynomial is given by*

$$G_\chi(x) = (x - 8^q)\prod_{i=0}^{q}(x - (2(1 + \sqrt{5}))^{q-i}(2(1 - \sqrt{5}))^i).$$

Proof. Let $\chi = 3q$ and let $3n = 3qk$. By Corollary 5.4, the weight of $f = 3\text{-}(1, 2, \chi + 1)_{3qk}$ is given by

$$\mathrm{wt}(f) = \frac{1}{2}(2^{3qk} - ((2(1 + \sqrt{5}))^l + (2(1 - \sqrt{5}))^l)^d), \tag{6.1}$$

where $d = \gcd(n, \chi/3) = \gcd(qk, q) = q$ and $l = n/d = qk/q = k$. We note that d does not change as the number of variables in f increases and that l increases with k. We can rewrite (6.1) as

$$\begin{aligned}\mathrm{wt}(f) &= \frac{1}{2}(8^{qk} - ((2(1 + \sqrt{5}))^k + (2(1 - \sqrt{5}))^k)^q)\\ &= \frac{1}{2}\Big((8^q)^k - \sum_{i=0}^{q}\binom{q}{i}((2(1 + \sqrt{5}))^k)^{q-i}((2(1 - \sqrt{5}))^k)^i\Big)\\ &= \frac{1}{2}\Big((8^q)^k - \sum_{i=0}^{q}\binom{q}{i}((2(1 + \sqrt{5}))^{q-i})^k((2(1 - \sqrt{5}))^i)^k\Big).\end{aligned} \tag{6.2}$$

Thus, for any χ, we can determine the k-th crucial weight of χ, say a_k, by

$$a_k = \sum_{i=1}^{q+1} -\frac{c_i}{2}\alpha_i^k + \frac{1}{2}8^{qk}, \tag{6.3}$$

where the α_i are the $(2(1+\sqrt{5}))^{q-i}(2(1-\sqrt{5}))^i$ terms from (6.2) and the c_i are their associated binomial coefficients. By the theory of recursions, then the numbers $8^q, \alpha_0, \ldots, \alpha_q$ are the roots of the recursion polynomial for the crucial weights, and so our recursion polynomial is the one given above, as required. □

We can expand on the above idea to prove the following theorem, which gives an explicit formula, including the roots, for the polynomials $F_\chi(x)$ defined in Section 4.

Theorem 6.4. *Let $\chi = 3q$. Then the sequence of weights $\mathrm{wt}(f_{3n,3q})$, $n = q+1, q+2, \ldots$ satisfies a recursion of order $q^2 - q + 3$ which has recursion polynomial*

$$F_\chi(x) = (x-8)(x^2-4x-16)\prod_{i=1}^{q-1}\prod_{j=1}^{q}\Big(x - \big((2(1+\sqrt{5}))^{q-i}(2(1-\sqrt{5}))^i\big)^{1/q}\zeta_q^j\Big),$$

where ζ_q is a primitive q-th root of unity.

Proof. First assume q is prime. If $n \neq kq$, Corollary 5.4 gives

$$\mathrm{wt}(f_{3n,3q}) = \frac{1}{2}\big(8^n - (2(1+\sqrt{5}))^n - (2(1-\sqrt{5}))^n\big). \tag{6.4}$$

For $n = kq$, on the other hand, by (6.3) we have

$$\mathrm{wt}(f_{3qk,3q}) = \sum_{i=1}^{q+1} -\frac{c_i}{2}\alpha_i^k + \frac{1}{2}8^k, \tag{6.5}$$

where the α_i are the $(2(1+\sqrt{5}))^{q-i}(2(1-\sqrt{5}))^i$ terms from (6.2) and the c_i are their associated binomial coefficients. We can combine (6.4) and (6.5) by multiplying (6.5) by $1/q\sum_{j=1}^{q}\zeta_q^{jn}$ where ζ_q is a primitive q-th root of unity. We also need to change the indices in (6.5) to match with the general n, so we let $k = n/q$. Finally, we note that for $n = qk$ the terms 8^{qk} and $(2(1\pm\sqrt{5}))^{qk}$ appear in both (6.4) and (6.5). To eliminate this overlap, we remove these terms from (6.5). Putting all of this together we have that

$$\mathrm{wt}(f_{3n,3q}) = \frac{1}{2}\big(8^n - (2(1+\sqrt{5}))^n - (2(1-\sqrt{5}))^n\big) + \Big(\frac{1}{q}\sum_{j=1}^{q}\zeta_q^{jn}\Big)\Big(\sum_{i=1}^{q-1} -\frac{c_i}{2}\alpha_i^{n/q}\Big). \tag{6.6}$$

Thus, by the theory of recursions, the $3 + q(q-1) = q^2 - q + 3$ terms in the above sum are the roots of the recursion polynomial for 3-f_{3q} and so the claim is proved.

The same result holds even if q is not prime. To see this, assume $d|q$ for some $d > 1$. This implies $\mathrm{wt}(f_{3n,3q}) = \mathrm{wt}(f_{3n,3d})$ for all $n \equiv 0 \bmod d$ but $n \not\equiv 0 \bmod q$. Thus, we begin by writing (6.6) and adding the terms from $\mathrm{wt}(f_{3n,3d})$:

$$\frac{1}{2}\big(8^n - (2(1+\sqrt{5}))^n - (2(1-\sqrt{5}))^n\big) + \underbrace{\Big(\frac{1}{d}\sum_{j=1}^{d}\zeta_d^{jn}\Big)\Big(\sum_{i=1}^{d-1} -\frac{c_i}{2}\alpha_i^{n/d}\Big)}_{S_d} + \underbrace{\Big(\frac{1}{q}\sum_{j=1}^{q}\zeta_q^{jn}\Big)\Big(\sum_{i=1}^{q-1} -\frac{c_i}{2}\alpha_i^{n/q}\Big)}_{S_q}. \tag{6.7}$$

In what follows, we will refer to the first sums in (6.7) as S_d and the second as S_q, as labeled above. Now, observe that if $q = dp$, then all of the d-th roots of unity are also q-th roots of unity (since $\zeta_d^q = (\zeta_d^d)^p = 1^p = 1$). Next, we note that

$$\begin{aligned}\big((2(1+\sqrt{5}))^{d-i}(2(1-\sqrt{5}))^i\big)^{n/d} &= \big((2(1+\sqrt{5}))^{d-i}(2(1-\sqrt{5}))^i\big)^{pn/q}\\ &= \big((2(1+\sqrt{5}))^{p(d-i)}(2(1-\sqrt{5}))^{pi}\big)^{n/q}\\ &= \big((2(1+\sqrt{5}))^{q-pi}(2(1-\sqrt{5}))^{pi}\big)^{n/q}.\end{aligned}$$

Thus, each of the terms from S_d is already present in S_q, so when we added S_d to (6.6) we did not add any new roots α_j, we merely adjusted the coefficients of the terms in (6.6). We note that this also implies that (6.7) has some redundancy in its roots. To compensate, we must reduce the size of the c_i for all α_i in S_q that also appear in S_d.

Repeating the above argument for all factors of q, we can see that no new α_i's are added and that the coefficients of the existing ones change with each iteration. Thus, the weight of $f_{3n,\chi}$ is given by a weighted sum of the elements in S_q, 8^n, and $(2(1 \pm \sqrt{5}))^n$. So, by the theory of recursions, we have that the weights for $f_{3k,\chi}$ satisfy a recursion which has recursion polynomial

$$(x-8)(x-(2(1+\sqrt{5})))(x-(2(1-\sqrt{5})))\prod_{i=1}^{q-1}\prod_{j=1}^{q}(x-(\alpha_i)^{1/q}\zeta_q^j),$$

where the α_i are as defined above and ζ_q is a primitive q-th root of unity. The degree of the above polynomial (and hence the degree of the recursion) is $3 + q(q-1) = q^2 - q + 3$, as required. □

Corollary 6.5. *If $\chi(1)$ and $\chi(2)$ are $3u$ and $\chi(1)$ divides $\chi(2)$, then $F_{\chi(1)}(x)$ divides $F_{\chi(2)}(x)$.*

Example 6.6. Let $\chi = 12 = 3 \cdot 4$. In this case, $q = 4$, which has one nontrivial divisor $d = 2$. From (6.7) we have

$$\begin{aligned}
\mathrm{wt}(f_{3n,12}) &= \frac{1}{2}\Big(8^n - (2(1+\sqrt{5}))^n - (2(1-\sqrt{5}))^n - (1^n+(-1)^n)\big((2(1+\sqrt{5}))(2(1-\sqrt{5}))\big)^{n/2}\Big)\\
&\quad - \frac{1}{4}(1^n+(-1)^n+i^n+(-i)^n)\Big(2\big((2(1+\sqrt{5}))^3(2(1-\sqrt{5}))\big)^{n/4}\\
&\quad + 3\big((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2\big)^{n/4} + 2\big((2(1+\sqrt{5}))(2(1-\sqrt{5}))^3\big)^{n/4}\Big) - E\\
&= \frac{1}{2}\Big(8^n - (2(1+\sqrt{5}))^n - (2(1-\sqrt{5}))^n - (1^n+(-1)^n)\big((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2\big)^{n/4}\Big)\\
&\quad - \frac{1}{4}(1^n+(-1)^n+i^n+(-i)^n)\Big(2\big((2(1+\sqrt{5}))^3(2(1-\sqrt{5}))\big)^{n/4}\\
&\quad + 3\big((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2\big)^{n/4} + 2\big((2(1+\sqrt{5}))(2(1-\sqrt{5}))^3\big)^{n/4}\Big) - E,
\end{aligned}$$

where E represents the repeated terms. Note that, when $n = 4k$, we have an extra copy of

$$\big((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2\big)^k,$$

so we see that $E = ((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2)^k$. Thus

$$\begin{aligned}
\mathrm{wt}(f_{3n,12}) &= \frac{1}{2}\Big(8^n - (2(1+\sqrt{5}))^n - (2(1-\sqrt{5}))^n - (1^n+(-1)^n)\big((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2\big)^{n/4}\Big)\\
&\quad - \frac{1}{4}(1^n+(-1)^n+i^n+(-i)^n)\Big(2\big((2(1+\sqrt{5}))^3(2(1-\sqrt{5}))\big)^{n/4}\\
&\quad + 2\big((2(1+\sqrt{5}))^2(2(1-\sqrt{5}))^2\big)^{n/4} + 2\big((2(1+\sqrt{5}))(2(1-\sqrt{5}))^3\big)^{n/4}\Big).
\end{aligned}$$

So the recursion polynomial for $\chi = 12$ is

$$\begin{aligned}
F_{12} &= (x-8)(x^2-4x-16)\prod_{k=1}^{3}\prod_{j=1}^{4}\Big(x-\big((2(1+\sqrt{5}))^{4-k}(2(1-\sqrt{5}))^k\big)^{1/4}(i)^j\Big)\\
&= x^{15} - 12x^{14} + 16x^{13} + 128x^{12} + 512x^{11} - 6144x^{10} + 8192x^9 + 65536x^8 - 131072x^7 + 1572864x^6\\
&\quad - 2097152x^5 - 16777216x^4 - 16777216x^3 + 201326592x^2 - 268435456x - 2147483648.
\end{aligned}$$

This polynomial matches the results from Table 2 and $\deg(F_{12}) = 15 = 4^2 - 4 + 3 = q^2 - q + 3$, as required.

7 Powers of Lucas numbers

The sequence $L = \{\ell_n : n = 1, 2, \ldots\}$ of Lucas numbers is defined by $\ell_1 = 1$, $\ell_2 = 3$, $\ell_n = \ell_{n-1} + \ell_{n-2}$, $n = 3, 4, \ldots$. If we let the sequence $\{a_n : n = 1, 2, \ldots\}$ of Fibonacci numbers be defined by $a_1 = a_2 = 1$, $a_n = a_{n-1} + a_{n-2}$, $n = 3, 4, \ldots$ and we define

$$\gamma = 1 + \sqrt{5}, \quad \delta = 1 - \sqrt{5}, \tag{7.1}$$

	$L_m(x)$
$m = 1$	$x^2 - x - 1$
$m = 2$	$x^3 - 2x^2 - 2x + 1$
$m = 3$	$x^4 - 3x^2 - 6x^2 + 3x + 1$
$m = 4$	$x^5 - 5x^4 - 15x^3 + 15x^2 + 5x - 1$
$m = 5$	$x^6 - 8x^5 - 40x^4 + 60x^3 + 40x^2 - 8x - 1$
$m = 6$	$x^7 - 13x^6 - 104x^5 + 260x^4 + 260x^3 - 104x^2 - 13x + 1$

Table 3. List of $m : L_m(x)$.

then it is easy to see that

$$\ell_n = \frac{1}{2^n}(\gamma^n + \delta^n) \quad \text{and} \quad a_n = \frac{1}{2^n\sqrt{5}}(\gamma^n - \delta^n), \quad n = 1, 2, \ldots. \tag{7.2}$$

The next theorem gives a simple formula for the crucial Walsh values in terms of powers of the Lucas numbers.

Theorem 7.1. *The crucial Walsh values $W_{k\chi/3,\chi}$ satisfy*

$$W_{k\chi/3,\chi} = (4^k\ell_k)^{\chi/3}, \quad n = 2, 3, \ldots.$$

Proof. It follows from (7.1) and Corollary 5.4 (note $3n = k\chi$, $d = \chi/3$ and $\ell = k$) that

$$\mathrm{wt}(f_{k\chi,\chi}) = \frac{1}{2}\big(2^{k\chi} - (4^k(\gamma^k + \delta^k))^{\chi/3}\big), \quad k = 2, 3, \ldots.$$

Now (4.1) and (7.2) give the theorem. □

Corollary 7.2. *For $\chi = 3$, the sequence of Walsh values $W_{n,3}$, $n = 2, 3, \ldots$ satisfies*

$$W_{n,3} = 4^n\ell_n, \quad n = 2, 3, \ldots, \tag{7.3}$$

so for any χ the crucial Walsh values satisfy

$$W_{n\chi/3,\chi} = (W_{n,3})^{\chi/3}, \quad n = 2, 3, \ldots. \tag{7.4}$$

The theory of recursions for powers of Fibonacci and Lucas numbers (and indeed for powers of other sequences defined by linear recursion of order 2) was developed long ago (see [5, 14, 21]) and we can use some of those results to obtain more information about the recursion polynomial for the crucial Walsh value sequences $Cv(\chi)$; let $V_\chi(x)$ denote this polynomial. It is clear from (4.1) and Lemma 6.3 that

$$V_\chi(x) = G_\chi(x)/(x - 8^q). \tag{7.5}$$

Theorem 7.1 shows that the crucial Walsh values $Cv(\chi)$ are just the $\chi/3$-th powers of the sequence $4^k\ell_k$, $k = 2, 3, \ldots$. The recursion polynomials for the powers of the Lucas numbers are given in the following lemma. The first few recursion polynomials are listed in Table 3.

Lemma 7.3. *The sequence ℓ_k^m, $k = 2, 3, \ldots$, of m-th powers of the Lucas numbers satisfies a linear recursion of order $m + 1$ with polynomial*

$$L_m(x) = \sum_{i=0}^{m+1} (-1)^{i(i+1)/2} \begin{bmatrix} m+1 \\ i \end{bmatrix} x^i, \tag{7.6}$$

where $\begin{bmatrix} m \\ i \end{bmatrix}$ is the Fibonomial coefficient $a_m a_{m-1} \cdots a_{m-i+1}/a_i a_{i-1} \cdots a_1$, $\begin{bmatrix} m \\ 0 \end{bmatrix} = 1$.

Proof. This is a special case of results of [5, Section 6] and [14, (50), p. 443], and perhaps goes back farther. □

	$V_\chi(x)$
$\chi = 3$	$x^2 - 4x - 16$
$\chi = 6$	$x^3 - 32x^2 - 512x + 4096$
$\chi = 9$	$x^4 - 192x^3 - 24576x^2 + 786432x + 16777216$
$\chi = 12$	$x^5 - 1280x^4 - 983040x^3 + 251658240x^2 + 21474836480x - 1099511627776$

Table 4. List of $\chi : V_\chi(x)$.

	$\chi = 3$	$\chi = 6$	$\chi = 9$	$\chi = 12$
$n = 3$	$4*$			
$n = 6$	$48*$	$16*$		
$n = 9$	$256*$	256	$64*$	
$n = 12$	$1792*$	$2304*$	1792	256
$n = 15$	$11264*$	11264	11264	11264
$n = 18$	$73728*$	$65536*$	65536	65536
$n = 21$	$475136*$	475136	475136	475136
$n = 24$	$3080192*$	$3211264*$	3080192	$5308416*$
$n = 27$	$19922944*$	19922944	$16777216*$	19922944
$n = 30$	$128974848*$	$126877696*$	128974848	126877696
$n = 33$	$834666496*$	834666496	834666496	834666496
$n = 36$	$5402263552*$	$5435817984*$	$5754585088*$	$4294967296*$
$n = 39$	$34963718144*$	34963718144	34963718144	34963718144
$n = 42$	$226291089408*$	$225754218496*$	226291089408	225754218496
$n = 45$	$1464583847936*$	1464583847936	$1429150367744*$	1464583847936

Table 5. Some values of $W_{n,\chi}$ for $3 \le \chi \le 12$.

By Theorem 7.1, if we multiply x^i in (7.6) with $m = \chi/3$ by $4^{(\chi/3)(m+1-i)}$, we must get the polynomial $V_\chi(x)$, that is,

$$V_\chi(x) = \sum_{i=0}^{(\chi/3)+1} (-1)^{i(i+1)/2} \begin{bmatrix} (\chi/3)+1 \\ i \end{bmatrix} 4^{(\chi/3)((\chi/3)+1-i)} x^i.$$

If we make this calculation, we get Table 4; of course this also follows from (7.5).

There are now several options for computing Walsh values $W_{n,\chi}$ (or, equivalently, weights, by (4.1)). One can use the recursion polynomial $F_\chi(x)$, but this requires finding the initial values for the recursion and would give a lengthy calculation if n is large. One can compute $W_{n,3}$ from (7.3) and then simply use (7.4) if $W_{n,\chi}$ is a crucial value. If not, then $W_{n,\chi}$ is a crucial value in the sequence $W_{k\chi'/3,\chi'}$ for some $\chi' < \chi$, by Lemma 6.2. Table 5 illustrates the simple distribution of the crucial Walsh values, which are followed by $*$. Of course the table could be extended to give entries for $n \le \chi$, where the numbers $W_{n,\chi}$ are not defined, by simply using the polynomials $F_\chi(x)$ to calculate those values near the top of the table. In the table we have done this only for $n = \chi$.

References

[1] M. L. Bileschi, T. W. Cusick and D. Padgett, Weights of Boolean cubic monomial rotation symmetric functions, *Cryptogr. Commun.* **4** (2012), 105–130.

[2] A. Brown and T. W. Cusick, Recursive weights for some Boolean functions, *J. Math. Cryptol.* **6** (2012), 105–135.

[3] A. Brown and T. W. Cusick, Equivalence classes for cubic rotation symmetric functions, *Cryptogr. Commun.* **5** (2013), 85–118.

[4] C. Carlet, G. Gao and W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions, *J. Combin. Theory Ser. A* **127** (2014), 161–175.

[5] L. Carlitz, Generating functions for powers of a certain sequence of numbers, *Duke Math. J.* **29** (1962), 521–537.

[6] T. W. Cusick, Affine equivalence of cubic homogeneous rotation symmetric Boolean functions, *Inform. Sci.* **181** (2011), 5067–5083.
[7] T. W. Cusick, Permutation equivalence of cubic rotation symmetric Boolean functions, *Int. J. Comput. Math.* (2014), DOI 10.1080/00207160.2014.964693.
[8] T. W. Cusick and A. Brown, Affine equivalence for rotation symmetric Boolean functions with p^k variables, *Finite Fields Appl.* **18** (2012), 547–562.
[9] T. W. Cusick and Y. Cheon, Affine equivalence of quartic homogeneous rotation symmetric Boolean functions, *Inform. Sci.* **259** (2014), 192–211.
[10] T. W. Cusick and B. Johns, Theory of 2-rotation symmetric cubic Boolean functions, *Des. Codes Cryptogr.* (2014), DOI 10.1007/s10623-014-9964-2.
[11] T. W. Cusick and D. Padgett, A recursive formula for weights of Boolean rotation symmetric functions, *Discrete Appl. Math.* **160** (2011), 391–397.
[12] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions*, Academic Press, San Diego, 2009.
[13] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, American Mathematical Society, Providence, 2003.
[14] A. F. Horadam, Generating functions for powers of a certain generalised sequence of numbers, *Duke Math. J.* **32** (1965), 437–446.
[15] S. Kavut, Results on rotation-symmetric S-boxes, *Inform. Sci.* **201** (2012), 93–113.
[16] S. Kavut, S. Maitra and M. D. Yücel, Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240, in: *Indocrypt 2006*, Lecture Notes in Comput. Sci. 4329, Springer, Berlin (2006), 266–279.
[17] S. Kavut, S. Maitra and M. D. Yücel, Search for Boolean functions with excellent profiles in the rotation symmetric class, *IEEE Trans. Inform. Theory* **53** (2007), 1743–1751.
[18] S. Kavut and M. D. Yücel, Generalized rotation symmetric and dihedral symmetric boolean functions – 9 variable boolean functions with nonlinearity 242, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (AAECC 2007), Lecture Notes in Comput. Sci. 485, Springer, Berlin (2007), 321–329.
[19] S. Kavut and M. D. Yücel, 9-variable boolean functions with nonlinearity 242 in the generalized rotation symmetric class, *Inform. and Comput.* **208** (2010), 341–350.
[20] H. Kim, S.-M. Park and S. G. Hahn, On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2, *Discrete Appl. Math.* **157** (2009), 428–432.
[21] J. Riordan, Generating functions for powers of Fibonacci numbers, *Duke Math. J.* **29** (1962), 5–12.

Received May 10, 2014; revised October 22, 2014; accepted November 23, 2014.